STATEMENT OF

BARBARA LAWLER

CHIEF PRIVACY OFFICER

HEWLETT-PACKARD COMPANY

BEFORE THE

COMMERCE, SCIENCE AND TRANSPORTATION COMMITTEE
UNITED STATES SENATE

FEDERAL PRIVACY LEGISLATION

APRIL 25, 2002

Mr. Chairman, Members of the Committee, I thank you for the invitation to appear today to discuss the need for stronger federal protections for consumer privacy, and comment specifically on S.2201.

My name is Barbara Lawler, and as the HP Privacy Manager, I have global responsibility for Hewlett-Packard's privacy policy management, implementation, compliance, education and communication, in both the online and offline worlds.

By way of background, HP is a leading provider of computing and imaging solutions and services. As a company we are focused on making technology and its benefits accessible to individuals and businesses through networked appliances, beneficial e-services and an '"always on" Internet infrastructure.

As a high-tech company that sells to the consumer market, we are deeply committed to strong privacy practices. HP believes that self-regulation with credible third-party enforcement -- such as the Better Business Bureau privacy seal program -- is the single most important step that businesses can take to ensure that consumers' privacy will be respected and protected online. We have also felt for some time, that there must be a 'floor' of uniform consumer privacy protections which all companies must adhere to. HP has testified on a number of occasions before Congress about our support for strong, practicable, federal privacy protections. We at HP have had much experience in developing and managing consumer-friendly privacy policies and practices, so we welcome the opportunity to share our experiences with the Committee about what we think works –and what may not work—in crafting privacy standards.

We want to commend you, Mr. Chairman, the ranking minority Member (Senator McCain), and the other Members of the Committee for your commitment to finding solutions to address consumer concerns about protecting their privacy. Three years ago, when HP first advocated the need for a federal initiative on privacy, we were virtually alone as a corporation in advocating that position. We think times have changed, and that many more companies and associations will support reasonable, baseline federal legislation for protecting consumers' privacy. It is time –past time—to develop national privacy standards. We welcome your leadership in working through the difficult issues that must be resolved if we are to see privacy legislation enacted this year, and we welcome your bill, Mr. Chairman, as a starting point for those discussions.

Let me start by giving you an overall picture of how we manage privacy at Hewlett-Packard. HP applies a universal, global privacy policy built on the fair information practices: notice, choice, accuracy & access, security and oversight. Whether in English, French or Japanese, the core commitments are the same, with minimal localization required to reflect local country laws. Key elements of

our policy include no selling of customer data, no sharing of customer data outside HP without customer permission, customer access to core contact data and a customer feedback mechanism. We insist through contractual obligations that suppliers must abide by our policy. Our consumer business requires opt-in for email contact and our B2B business is moving to opt-in as well.

The HP policy can be viewed in its online form at the lower left-hand corner of every hp.com web page: http://www.welcome.hp.com/country/us/eng/privacy.htm

The guiding principles for managing data privacy at HP are:

- customers control their own personal data
- give customers choices that enhance trust and therefore enhance the business
- put the customer in the lead to determine how HP may use information about them; and
- have the highest integrity in practices, responses and partners

HP people apply the privacy policy to marketing, support, e-services and product generation using a set of HP-developed tools called the “Privacy Rulebook” and the “Web Site Data and Privacy Practices Self-Assessment Tool”.

A sample of current HP global privacy initiatives include:

- company-wide training on implementing privacy standards
- new application development and business rules for company-wide multiple customer database consolidation
- Platform for Privacy Preferences (P3P) implementation for our most active web sites
- Supplier contract compliance assessments

I want to underscore some important distinctions around the ‘opt-in’ discussion and add some clarity. It’s HP policy to never sell or share our customer data without their express permission. HP has many business relationships with other companies. Companies that act as service providers or suppliers to HP are contractually required through a Confidential Non-Disclosure Agreement and Personal Data Protection Agreement to abide by HP’s privacy policy.

HP’s strategic partnerships and co-marketing partners comprise a different class of business relationships. It is these relationships to which the HP opt-in policy requirement described above applies.

Applying the opt-in standard for marketing contact within HP is an order of magnitude more difficult, but we’re committed because it’s the right thing to do for our customers. Implementing opt-in for marketing contact requires us to evaluate all customer databases and customer privacy choice data elements, re-engineer

the data structures, systems and associated processes, change the privacy question format itself, develop implementation guides and tools, and communicate the new standard HP-wide. Some of the challenges we face are in the areas of managing a program-specific customer privacy choice with a 'top-down' HP request and resolving a large volume of data where the privacy choice is unknown.

On January 29th, 2001, HP became the first high-tech company to certify with the U.S. Department of Commerce for Safe Harbor. This demonstrates our continued leadership to strong privacy practices in the U.S. The Safe Harbor framework offers consistency and continuity for business operations conducted between HP sites located in the United States and the European Union; this is critical for a global enterprise. And because HP manages a global privacy policy, citizens in the U.S. enjoy the same benefits as those in the EU and elsewhere.

Finally, I would like to put the privacy issue into the larger perspective of consumer confidence in the global electronic marketplace. While consumers are concerned about their privacy online, they are also concerned about whether their credit cards are safe online, and whether if they order a blue vase from a website in Paris or Tokyo, they will get what they order in the quality and condition they expected. In order for online businesses to truly earn the trust of consumers, we need to expand ongoing efforts to make sure that the global electronic marketplace is a clean, well-lighted venue for both consumers and businesses. For example, consumers need to have confidence that when they do business across national borders, there will be a redress system in place should anything go wrong with the transaction.

HP is working with 70+ businesses from around the world through the Global Business Dialogue for electronic commerce to develop a consensus on worldwide standards on consumer redress systems, that is of Alternative Dispute Resolution (ADR). In this effort, we are working with consumer groups and the FTC and the European Commission so that consumers and businesses will be able to quickly, fairly and efficiently resolve complaints related to online transactions.

I would now like to turn to the language of S. 2201.

First of all, we are pleased that the bill bases its "Notice and Consent" requirements upon "clear and conspicuous" disclosure. HP has always felt that informed choice depends upon consumers having available the material information they need to make an informed choice with whom they wish to share their personal information. "Clear and conspicuous" is a term of art used by the FTC to provide robust notification, and we are pleased that Section 102 recognizes the importance of requiring this basic consumer protection. We are also pleased that there is a place in the legislation for privacy enhancing

technologies such as P3P, which enhance notice and support capabilities for consumers.

We are also pleased that the legislation does not take an 'either-or' stance on the opt-in, opt-out debate. We think the continued free flow of non-sensitive data, with the resulting economic benefits for both consumers and businesses, will be best served by an opt-out requirement and allowing room for competitive differentiation. For personally identifiable information that is of a sensitive nature (as defined by S.2201), an opt-in requirement will most likely give consumers greater confidence in participating in online transactions. HP believes a very constructive discussion can be held as to where the demarcation should be made between opt-in and opt-out.

We agree that as a general rule, the consent or denial of a consumer for permission to collect or disclose personally identifiable information should remain in effect until the consumer decides to change their preference.

We also agree on the importance of giving consumers reasonable data access to evaluate the accuracy of information collected. An observation we would make is that from our experience, data access can be a complex process. Many companies have multiple databases that collect data from a number of sources and mediums, and which may not be interoperable. Merging these data files is a prolonged, expensive process, though a process that is underway throughout industry.

A commensurate problem is that of authentication. Ensuring that someone is indeed who they say they are when they request access may bleed into security and identity theft issues. Creating a security breech or an identity theft problem while trying to address the access issue is a real concern.

Having said that, we would like to work with the Committee to find practicable, secure and cost-effective, solutions to the problems of access.

As to enforcement, we are pleased that the legislation recognizes the importance of the role of the FTC. Utilizing clear statutory parameters, we welcome an FTC rulemaking that will allow an opportunity to develop implementation rules and to help define with greater specificity the terms of the legislation. We also agree that there is a role for the state Attorneys General in the enforcement of this legislation, and we concur with the balance achieved in the bill, between the rights of states to protect their citizens, and the right of the FTC -- as the expert agency -- to interpret its rule.

One suggestion we would make, is to find a role for self-regulatory privacy seal programs that have standards equal or above those required under this legislation. As we have stated, we belong to the BBB privacy program, which we believe is quite strict, and which requires that any consumer complaint must be

addressed through a dispute resolution process. The more eyes and ears available to resolve privacy disputes will benefit consumers, and allowing the FTC to certify reputable seal programs to take a first crack at resolving disputes would be beneficial.

Turning to areas of the bill where we have concerns, we must state our strong opposition to the concept of a private right of action for a privacy violation. We agree with the legislation that there need to be strong, bright lines as to what businesses must do to protect their customers' privacy. As we have said, we welcome a healthy debate on opt-in and opt-out; we welcome FTC and state Attorneys General enforcement, and we would urge the Committee to consider adding language that will allow reputable seal programs to help in protecting consumer privacy. All of these initiatives add clarity and certainty to the job of protecting consumer privacy. We are concerned that a private right of action will create less certainty and clarity in the marketplace, as each court will supply its own definition as to what constitutes "actual harm" or "reasonable access" or "reasonable security". Calibrating "actual monetary loss" from privacy violations will therefore be an art rather than a science, as on each case, each court, and each plaintiff lawyer having their own view of the matter.

Consumers deserve adequate protections, and this bill -- as we have described -- fills a void in privacy protections. At the same time, businesses need certainty as to the rules of the road, so that they can meet the obligations required to address privacy issues. A private right of action in this dynamic environment places this need for clarity and certainty on its head; legislation with a private right of action will offer consumers and businesses less certainty at a time when we need more clarity as to what should be the national, uniform privacy compact.

On other issues addressed in the bill, we believe that there must be a recognition that the off-line world and on-line world should be subject to the same privacy rules. We would be pleased to work with the Committee in addressing that need for convergence recognizing the differences in offline and online implementation.

We also believe that "Whistleblower" law should be uniform across industries and therefore not considered for inclusion in this bill. Industry should not be piecemealed by variations in employment law relating to whistleblowers. And again, -- for the reasons stated above -- we are concerned about a private right of action included in the Whistleblower section.

Thank you Mr. Chairman for the opportunity to testify on S. 2201. HP looks forward to working with the Committee in developing -- and passing -- practicable consumer privacy protection, this Congress. I would be pleased to answer any questions that you may have.